UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/656,551	09/05/2003	Diana K. Smetters	PARC-DA3162Q	8170

35699   7590   05/09/2008

PVF -- PARC
c/o PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER
NGUYEN, KHAI MINH

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *13 March 2008*.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-25* is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-25* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a) ☐ All   b) ☐ Some * c) ☐ None of:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/15/2008*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

Response to Amendment

1.   Applicant's arguments with respect to claims 1-25 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Balfanz et al. (Talking to Strangers: Authentication in Ad-Hoc Wireless Networks) in

view of Hermann, Reto (EP 1024626) and further in view of Lowensohn et al. (U.S.Pub-

20040230809).

Regarding claim 1, Balfanz teaches a computer controlled method comprising:

establishing communication between a wireless sensor (item A) and a

provisioning device (Item B) over at least one preferred channel (fig.3, section 3.2, [2]),

said wireless sensor configured to send a first commitment to said provisioning device

over said at least one preferred channel (fig.3, [2]-[3]) and to receive a second

commitment from said provisioning device over said at least one preferred channel

(fig.3, [2]-[3]);

receiving <u>at least one</u> of provisioning information <u>or additional application-specific</u> <u>information, site-specific information, network-specific information, or other information</u> <u>that can be used by the wireless sensor</u> from said provisioning device over said at least one preferred channel (not specifically disclose), wherein the provisioning information includes a credential (fig.3, [2]-[3]) and wherein the credential facilitates becoming a member of a secure credential infrastructure (fig.5, section 4.1, [1]-[2]); and

Balfanz fails to specifically disclose receiving <u>at least one</u> of provisioning information <u>or additional application-specific information, site-specific information,</u> <u>network-specific information, or other information that can be used by the wireless</u> <u>sensor</u> from said provisioning device over said at least one preferred channel. However, Hermann teaches receiving <u>at least one</u> of provisioning information ([0020]) <u>or</u> <u>additional application-specific information, site-specific information, network-specific</u> <u>information, or other information that can be used by the wireless sensor</u> from said provisioning device over said at least one preferred channel (secure channel) ([0021]). It would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teaching of Hermann to Balfanz to prevent any accidental information exchange.

Balfanz and Hermann fail to specifically disclose automatically configuring said wireless sensor for transmitting sensor information over a secure communication channel responsive to said provisioning information. However, Lowensohn teaches automatically configuring said wireless sensor (fig.1, barb badge 100) for transmitting

sensor information over a secure communication channel responsive to said

provisioning information (fig.1, and 4, [0009]-[0010], [0059]). It would have been obvious

to one having ordinary skill in the art at the time the invention was made to apply the

teaching of Lowensohn to Balfanz and Hermann to detect the user orientation in the

environment and security the information of user.

Regarding claim 2, Balfanz, Hermann, and Lowensohn further teach the

computer controlled method of claim 1, wherein said provisioning information comprises

a credential (see Lowensohn, [0038], [0043]).

Regarding claim 3, Balfanz, Hermann, and Lowensohn further teach the

computer controlled method of claim 1, wherein said provisioning information further

comprises one or more of patient data, limit data, alarm data, dosage data, interval

data, access data, physician data, caregiver data, nurse data, insurance data or room

assignment data (see Lowensohn, fig.4, [0004], [0059]).

Regarding claim 4, Balfanz, Hermann, and Lowensohn further teach the

computer controlled method of claim 3, further comprising transmitting said sensor

information over said secure communication channel (see Lowensohn, fig.1, [0009],

[0271]).

Regarding claim 5, Balfanz, Hermann, and Lowensohn further teach the

computer controlled method of claim 1, wherein said provisioning information further

comprises one or more of sensitivity data, target data, image recognition data, or noise

characteristics (see Lowensohn, [0038], [0043]).

Regarding claim 6, Balfanz, Hermann, and Lowensohn further teach the
computer controlled method of claim 1, wherein said wireless sensor senses one or
more of medical information, location information, proximity information, environmental
information, or vehicle information (see Lowensohn, [0043]-[0044]).

Regarding claim 7, Balfanz teaches a computer-readable storage medium storing
instructions that when executed by a computer in a wireless sensor to cause the
computer to perform a method comprising steps of:

establishing communication between a wireless sensor and a provisioning device
over at least one preferred channel (fig.3, section 3.2, [2]), said wireless sensor
configured to send a first commitment to said provisioning device over said at least one
preferred channel (fig.3, [2]-[3]) and to receive a second commitment from said
provisioning device over said at least one preferred channel (fig.3, [2]-[3]);

receiving at least one of provisioning information or additional application-specific
information, site-specific information, network-specific information, or other information
that can be used by the wireless sensor from said provisioning device over said at least
one preferred channel (not specifically disclose), wherein the provisioning information
includes a credential (fig.3, [2]-[3]) and wherein the credential facilitates becoming a
member of a secure credential infrastructure (fig.5, section 4.1, [1]-[2]); and

Balfanz fails to specifically disclose receiving at least one of provisioning
information or additional application-specific information, site-specific information,
network-specific information, or other information that can be used by the wireless

<u>sensor</u> from said provisioning device over said at least one preferred channel. However,

Hermann teaches receiving <u>at least one</u> of provisioning information ([0020]) <u>or</u>

<u>additional application-specific information, site-specific information, network-specific</u>

<u>information, or other information that can be used by the wireless sensor</u> from said

provisioning device over said at least one preferred channel (secure channel) ([0021]). It

would have been obvious to one having ordinary skill in the art at the time the invention

was made to apply the teaching of Hermann to Balfanz to prevent any accidental

information exchange.

Balfanz and Hermann fail to specifically disclose automatically configuring said

wireless sensor for transmitting sensor information over a secure communication

channel responsive to said provisioning information. However, Lowensohn teaches

automatically configuring said wireless sensor (fig.1, barb badge 100) for transmitting

sensor information over a secure communication channel responsive to said

provisioning information (fig.1, and 4, [0009]-[0010], [0059]). It would have been obvious

to one having ordinary skill in the art at the time the invention was made to apply the

teaching of Lowensohn to Balfanz and Hermann to detect the user orientation in the

environment and security the information of user.

<u>Regarding claim 8</u>, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 7, wherein said provisioning information

comprises a credential (see Lowensohn, [0038], [0043]).

Regarding claim 9, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 7, wherein said provisioning information

further comprises one or more of patient data, limit data, alarm data, dosage data,

interval data, access data, physician data, caregiver data, nurse data, insurance data or

room assignment data (see Lowensohn, fig.4, [0004], [0059]).

Regarding claim 10, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 9, further comprising transmitting said

sensor information over said secure communication channel (see Lowensohn, fig.1,

[0009], [0271]).

Regarding claim 11, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 7, wherein said provisioning information

further comprises one or more of sensitivity data, target data, image recognition data, or

noise characteristics (see Lowensohn, [0038], [0043]).

Regarding claim 12, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 7, wherein said wireless sensor senses

one or more of medical information, location information, proximity information,

environmental information, or vehicle information (see Lowensohn, [0043]-[0044]).

Regarding claim 13, Balfanz teaches a wireless apparatus comprising:

at least one port configured to establish a preferred channel (fig.3, section 3.2,

[2]);

a preferred channel communication mechanism configured to be able to

establish communication with a provisioning device over said at least one preferred

channel (fig.3, section 3.2, [2]), said wireless sensor configured to send a first

commitment to said provisioning device over said at least one preferred channel (fig.3,

[2]-[3]) and to receive a second commitment from said provisioning device over said at

least one preferred channel (fig.3, [2]-[3]);

a receiver mechanism configured to be able to receive receiving <u>at least one</u> of

provisioning information <u>or additional application-specific information, site-specific</u>

<u>information, network-specific information, or other information that can be used by the</u>

<u>wireless sensor</u> from said provisioning device over said at least one preferred channel

(not specifically disclose), wherein the provisioning information includes a credential

(fig.3, [2]-[3]) and wherein the credential facilitates becoming a member of a secure

credential infrastructure (fig.5, section 4.1, [1]-[2]); and

Balfanz fails to specifically disclose a receiver mechanism configured to be able

to receive receiving <u>at least one</u> of provisioning information <u>or additional application-</u>

<u>specific information, site-specific information, network-specific information, or other</u>

<u>information that can be used by the wireless sensor</u> from said provisioning device over

said at least one preferred channel. However, Hermann teaches a receiver mechanism

configured to be able to receive receiving <u>at least one</u> of provisioning information

([0020]) <u>or additional application-specific information, site-specific information, network-</u>

<u>specific information, or other information that can be used by the wireless sensor</u> from

said provisioning device over said at least one preferred channel (secure channel)

([0021]). It would have been obvious to one having ordinary skill in the art at the time

the invention was made to apply the teaching of Hermann to Balfanz to prevent any

accidental information exchange.

Balfanz and Hermann fail to specifically disclose an automatic configuration

mechanism to enable said wireless sensor to transmit sensor information over a secure

communication channel established responsive to said provisioning information.

However, Lowensohn teaches an automatic configuration mechanism to enable said

wireless sensor (fig.1, barb badge 100) to transmit sensor information over a secure

communication channel established responsive to said provisioning information (fig.1,

and 4, [0009]-[0010], [0059]). It would have been obvious to one having ordinary skill in

the art at the time the invention was made to apply the teaching of Lowensohn to

Balfanz and Hermann to detect the user orientation in the environment and security the

information of user.

Regarding claim 14, Balfanz, Hermann, and Lowensohn further teach the

apparatus of claim 13, wherein said provisioning information comprises a credential

(see Lowensohn, [0038], [0043]).

Regarding claim 15, Balfanz, Hermann, and Lowensohn further teach the

apparatus of claim 13, wherein said provisioning information further comprises one or

more of patient data, limit data, alarm data, dosage data, interval data, access data,

physician data, caregiver data, nurse data, insurance data, room assignment data,

sensitivity data, target data, image recognition data, activation data, or noise

characteristics (see Lowensohn, fig.4, [0004], [0059]).

Regarding claim 16, Balfanz, Hermann, and Lowensohn further teach the

apparatus of claim 15, further comprising a transmission mechanism configured to

transmit said sensor information over said secure communication channel (see

Lowensohn, fig.1, [0009], [0271]).

Regarding claim 17, Balfanz, Hermann, and Lowensohn further teach the

apparatus of claim 13, wherein wireless apparatus further comprises a sensor for

measuring said sensor information (see Lowensohn, [0009]-[0010], [0038], [0043]).

Regarding claim 18, Balfanz, Hermann, and Lowensohn further teach the

apparatus of claim 13, wherein said wireless sensor senses one or more of medical

information, location information, proximity information, environmental information, or

vehicle information (see Lowensohn, [0043]-[0044]).

Regarding claim 19, Balfanz, Hermann, and Lowensohn further teach the

apparatus of claim 13, wherein said sensor information is status information about the

apparatus (see Lowensohn, fig.1, and 14a, [0009]-[0010], [0037]).

Regarding claim 20, Balfanz, Hermann, and Lowensohn further teach the

computer controlled method of claim 1, wherein said at least one preferred channel

comprises a single preferred channel capable of communicating both from said wireless

sensor to said provisioning device (see Balfanz, fig.3, section 3.1, [2]-[3]) and from said

provisioning device to said wireless sensor (see Balfanz, fig.3, section 3.1, [2]-[3]).

Regarding claim 21, Balfanz, Hermann, and Lowensohn further teach the

computer controlled method of claim 1, wherein said at least one preferred channel

comprises two separate channels, including a first preferred channel capable of

communicating from said wireless sensor to said provisioning device (see Balfanz, fig.3,

section 3.1, [2]-[3]) and a second preferred channel capable of communicating from said

provisioning device to said wireless sensor (see Balfanz, fig.3, section 3.1, [2]-[3]).

Regarding claim 22, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 7, wherein said at least one preferred

channel comprises a single preferred channel capable of communicating both from said

wireless sensor to said provisioning device (see Balfanz, fig.3, section 3.1, [2]-[3]) and

from said provisioning device to said wireless sensor (see Balfanz, fig.3, section 3.1, [2]-

[3]).

Regarding claim 23, Balfanz, Hermann, and Lowensohn further teach the

computer-readable storage medium of claim 7, wherein said at least one preferred

channel comprises two separate channels, including a first preferred channel capable of

communicating from said wireless sensor to said provisioning device (see Balfanz, fig.3,

section 3.1, [2]-[3]) and a second preferred channel capable of communicating from said

provisioning device to said wireless sensor (see Balfanz, fig.3, section 3.1, [2]-[3]).

Regarding claim 24, Balfanz, Hermann, and Lowensohn further teach the apparatus of claim 13, wherein said at least one preferred channel comprises a single preferred channel capable of communicating both from said wireless sensor to said provisioning device (see Balfanz, fig.3, section 3.1, [2]-[3]) and from said provisioning device to said wireless sensor (see Balfanz, fig.3, section 3.1, [2]-[3]).

Regarding claim 25, Balfanz, Hermann, and Lowensohn further teach the apparatus of claim 13, wherein said at least one preferred channel comprises two separate channels, including a first preferred channel capable of communicating from said wireless sensor to said provisioning device (see Balfanz, fig.3, section 3.1, [2]-[3]) and a second preferred channel capable of communicating from said provisioning device to said wireless sensor (see Balfanz, fig.3, section 3.1, [2]-[3]).

Conclusion

3.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to KHAI M. NGUYEN whose telephone number is

(571)272-7923. The examiner can normally be reached on 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Vincent P. Harper can be reached on 571.272.7605. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VINCENT P. HARPER/
Supervisory Patent Examiner, Art Unit 2617

/Khai M Nguyen/
Examiner, Art Unit 2617   5/6/2008